UNCLASSIFIED

Microsoft IE Version 7

Version: 4

Release: 2

23 April 2010

STIG.DOD.MIL

Sort Order: Group ID (Vulid), ascending order
Notice: Developed by DISA for the DoD
Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System= SECRET Checklist
Top Secret System = SECRET Checklist

Group ID (Vulid): V-3427
Group Title: IE - Zones: Use Only Machine Settings
Rule ID: SV-28784r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI320
Rule Title: Internet Explorer is not configured to require consistent security zone settings to all users.

Vulnerability Discussion: This setting enforces consistent security zone settings to all users of the computer. Security Zones control browser behavior at various web sites and it is desirable to maintain a consistent policy for all users of a machine.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Value Name: Security_HKLM_only

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Security Zones: Use only machine settings" to "Enabled".

Group ID (Vulid): V-3428
Group Title: IE - Zones: Do Not Allow Users to Change Policies
Rule ID: SV-28782r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI319
Rule Title: Internet Explorer is configured to Allow Users to Change Policies.

Vulnerability Discussion: This setting prevents users from changing the Internet Explorer policies on the machine. Policy changes should be made by Administrators only, so this setting should be Enabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Value Name: Security_Options_Edit

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Security Zones: Do Not Allow Users to Change Policies” to “Enabled”.

Group ID (Vulid): V-3429
Group Title: IE - Zones: Do Not Allow Users to Add/Delete Sites
Rule ID: SV-28780r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI318
Rule Title: Internet Explorer is configured to Allow Users to Add/Delete Sites.

Vulnerability Discussion: This setting prevents users from adding sites to various security zones. Users should not be able to add sites to different zones, as this could allow them to bypass security controls of the system.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Value Name: Security_Zones_Map_Edit

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Security Zones: Do Not Allow Users to Add/Delete Sites” to “Enabled”.

Group ID (Vulid): V-3430
Group Title: IE - Make Proxy Settings Per Machine
Rule ID: SV-3430r10_rule
Severity: CAT III
Rule Version (STIG-ID): DTBI367
Rule Title: Internet Explorer is not configured to disable making Proxy Settings Per Machine.

Vulnerability Discussion: This setting controls whether or not the Internet Explorer proxy settings are configured on a per-user or per-machine basis.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Make proxy settings per-machine (rather than per user)” to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Criteria: If the value ProxySettingsPerUser is REG_DWORD = 1, this is not a finding.

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Make proxy settings per-machine (rather than per user)” to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Criteria: Set the value ProxySettingsPerUser to REG_DWORD = 1.

Group ID (Vulid): V-3431
Group Title: IE - Disable Automatic Install of IE Components
Rule ID: SV-28800r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI316
Rule Title: Internet Explorer is configured to allow Automatic Install of components.

Vulnerability Discussion: This setting controls the ability of Internet Explorer to automatically install components if it goes to a site that requires components that are not currently installed. The System Administrator should install all components on the system. If additional components are necessary, the user should inform the SA and have the SA install the components.

Responsibility: System Administrator
IAControls: DCSL-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Internet Explorer\InfoDelivery\Restrictions\

Value Name: NoJITSetup

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Disable Automatic Install of Internet Explorer components” to “Enabled”.

Group ID (Vulid): V-3432
Group Title: IE - Disable Periodic Check for IE Updates
Rule ID: SV-28778r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI317
Rule Title: Internet Explorer is configured to automatically check for updates.

Vulnerability Discussion: This setting determines whether or not Internet Explorer will periodically check the Microsoft web sites to determine if there are updates to Internet Explorer available. The SA should manually install all updates on a system so that configuration control is maintained.

Responsibility: System Administrator
IAControls: DCSL-1

Check Content:
If the following registry value doesn’t exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Internet Explorer\InfoDelivery\Restrictions\

Value Name: NoUpdateCheck

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Disable Periodic Check for Internet Explorer Software Updates” to “Enabled”.

Group ID (Vulid): V-6243
Group Title: DTBI022-Download signed Active X controls-Internet
Rule ID: SV-16439r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI022
Rule Title: Download signed ActiveX controls for internet zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether users may download signed ActiveX controls from a page in the zone. If you enable this policy, users can download signed controls without user intervention. If you select Prompt in the drop-down box, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded. If you disable the policy setting, signed controls cannot be downloaded. If you do not configure this policy setting, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1001 to REG_DWORD = 3.

Group ID (Vulid): V-6244
Group Title: DTBI023-Download unsigned ActiveX controls-Interne
Rule ID: SV-16441r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI023
Rule Title: Download unsigned ActiveX controls for internet zone is not disabled.

Vulnerability Discussion: Active X controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download unsigned ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1004 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Download unsigned ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1004 to REG_DWORD = 3.

Group ID (Vulid): V-6245

Group Title: DTBI024-Initialize and script ActiveX controls
Rule ID: SV-16443r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI024
Rule Title: Initialize and script ActiveX controls not marked as safe for internet zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage ActiveX controls not marked as safe.
If you enable this policy setting, ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option.
If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted. If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. If you do not configure this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1201 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1201 to REG_DWORD = 3.

Group ID (Vulid): V-6248
Group Title: DTBI030-Font download control - Internet Zone
Rule ID: SV-16435r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI030
Rule Title: Allow font downloads for internet zone is not disabled.

Vulnerability Discussion: Download of fonts can sometimes contain malicious code.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet

Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow font downloads" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1604 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow font downloads" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1604 to REG_DWORD = 3.

Group ID (Vulid): V-6249
Group Title: DTBI031-Java Permissions not set for Internet Zone
Rule ID: SV-16447r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI031
Rule Title: Java permissions for internet zone are not disabled.

Vulnerability Discussion: Java must have level of protections based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-6250
Group Title: DTBI032-Access data sources across domains-Interne
Rule ID: SV-16283r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI032
Rule Title: Access data sources across domains are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer can access data from another security zone using the Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO). If you enable this policy setting, users can load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you select Prompt in the drop-down box, users are queried to choose whether to allow a page to be loaded in the zone that uses MSXML or ADO to access data from another site in the zone. If you disable this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you do not configure this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Access data sources across domains" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1406 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Access data sources across domains" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria:Set the value 1406 to REG_DWORD = 3.

Group ID (Vulid): V-6253
Group Title: DTBI036-Drag and drop or copy and paste-Internet
Rule ID: SV-16433r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI036
Rule Title: The Allow drag and drop or copy and paste files for internet zone are not disabled.

Vulnerability Discussion: Drag and Drop of files must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet

Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow drag and drop or copy and paste files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value for 1802 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow drag and drop or copy and paste files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1802 to REG_DWORD = 3.

Group ID (Vulid): V-6254
Group Title: DTBI037-Installation of desktop items - Internet
Rule ID: SV-16437r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI037
Rule Title: Allow installation of desktop items for internet zone is not disabled.

Vulnerability Discussion: Installation of items must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow installation of desktop items" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1800 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow installation of desktop items" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1800 to REG_DWORD = 3.

Group ID (Vulid): V-6255
Group Title: DTBI038-Launching programs and files in IFRAME-Int
Rule ID: SV-16449r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI038
Rule Title: Launching applications and files in an IFRAME for internet zone is not disabled.

Vulnerability Discussion: Launching of programs in IFRAME must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Launching applications and files in an IFRAME" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1804 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Launching applications and files in an IFRAME" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1804 to REG_DWORD = 3.

Group ID (Vulid): V-6256
Group Title: DTBI039-Navigate sub-frames across domains-Interne
Rule ID: SV-16453r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI039
Rule Title: Navigate sub-frames across different domains for internet zone are not disabled.

Vulnerability Discussion: Frames that navigate across different domains are a security concern because the user may think they are accessing pages on one site while they are actually accessing pages on another site.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Navigate sub-frames across different domains" will be set to “Enabled" and then select "Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1607 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Navigate sub-frames across different domains" will be set to "Enabled“ and then select "Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1607 to REG_DWORD = 3.

Group ID (Vulid): V-6257
Group Title: DTBI040-Software channel permissions - Internet
Rule ID: SV-16455r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI040
Rule Title: Software channel permissions for internet zone are not disabled.

Vulnerability Discussion: Software Channel permissions must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Software channel permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1E05 is REG_DWORD = 65536, (Decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Software channel permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1E05 to REG_DWORD = 65536, (Decimal).

Group ID (Vulid): V-6259

Group Title: DTBI042-Userdata persistence - Internet Zone
Rule ID: SV-16457r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI042
Rule Title: Userdata persistence for internet zone is not disabled.

Vulnerability Discussion: Userdata persistence must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Userdata persistence" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1606 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Userdata persistence" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1606 to REG_DWORD = 3.

Group ID (Vulid): V-6260
Group Title: DTBI044-Allow paste operations via script-Internet
Rule ID: SV-16431r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI044
Rule Title: Allow cut, copy or paste operations from the clipboard via script are not disabled for internet zone.

Vulnerability Discussion: This policy setting allows you to manage whether scripts can perform a clipboard operation (for example, cut, copy, and paste) in a specified region.
If you enable this policy setting, a script can perform a clipboard operation.
If you select Prompt in the drop-down box, users are queried as to whether to perform clipboard operations. If you disable this policy setting, a script cannot perform a clipboard operation. If you do not configure this policy setting, a script can perform a clipboard operation.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1407 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1407 to REG_DWORD = 3.

Group ID (Vulid): V-6262
Group Title: DTBI046-User Authentication-Logon - Internet Zone
Rule ID: SV-16451r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI046
Rule Title: Logon options for internet zone are not enabled.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Logon options" will be set to “Enabled” and "Prompt for user name and password" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1A00 is REG_DWORD = 65536 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Logon options" will be set to “Enabled” and "Prompt for user name and password" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1A00 to REG_DWORD = 65536 (decimal).

Group ID (Vulid): V-6267
Group Title: DTBI061-Java Permissions not set - Local Zone
Rule ID: SV-16445r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI061
Rule Title: Java permissions for local intranet zone are not disabled.

Vulnerability Discussion: Java must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Intranet Zone -> "Java permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1C00 is REG_DWORD = 65536, (Decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Intranet Zone -> "Java permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: Set the value 1C00 to REG_DWORD = 65536, (Decimal).

Group ID (Vulid): V-6281
Group Title: DTBI091-Java Permissions not set - Trusted Sites
Rule ID: SV-16446r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI091
Rule Title: Java permissions for trusted sites zone are not disabled.

Vulnerability Discussion: Java must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Trusted Sites Zone -> "Java permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1C00 is REG_DWORD = 65536, (Decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Trusted Sites Zone -> "Java permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: Set the value 1C00 to REG_DWORD = 65536, (Decimal).

Group ID (Vulid): V-6289
Group Title: DTBI112-Download signed ActiveX - Restricted Sites
Rule ID: SV-16440r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI112
Rule Title: Download signed ActiveX controls for restricted sites zone is not disabled.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1001 to REG_DWORD = 3.

Group ID (Vulid): V-6290
Group Title: DTBI113-Download unsigned ActiveX - Restricted Sit
Rule ID: SV-16442r2_rule

Severity: CAT II
Rule Version (STIG-ID): DTBI113
Rule Title: Download unsigned ActiveX controls for restricted sites zone is not disabled.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download unsigned ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1004 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Download unsigned ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1004 to REG_DWORD = 3.

Group ID (Vulid): V-6291
Group Title: DTBI114-Initialize and script ActiveX - Restricted
Rule ID: SV-16444r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI114
Rule Title: Initialize and script ActiveX controls not marked as safe for restricted sites zone is not disabled.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked
safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to “Enabled” and "Disable" selected from down drop box.

Procedures: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1201 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Initialize and script ActiveX controls not marked as safe" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1201 to REG_DWORD = 3.

Group ID (Vulid): V-6292
Group Title: DTBI115-Run ActiveX controls and plugins-Restricte
Rule ID: SV-16464r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI115
Rule Title: Run ActiveX controls and plugins are not disabled..

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked
safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run ActiveX controls and plugins" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1200 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run ActiveX controls and plugins" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1200 to REG_DWORD = 3.

Group ID (Vulid): V-6293
Group Title: DTBI116-Script ActiveX controls marked safe-Restri

Rule ID: SV-16465r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI116
Rule Title: Script ActiveX controls marked safe for scripting is not disabled.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked
safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Script ActiveX controls marked safe for scripting" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1405 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Script ActiveX controls marked safe for scripting" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1405 to REG_DWORD = 3.

Group ID (Vulid): V-6294
Group Title: DTBI119-File download control - Restricted Sites
Rule ID: SV-16462r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI119
Rule Title: Allow file downloads are not disabled.

Vulnerability Discussion: Files should not be able to be downloaded from sites that are considered restricted.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow file downloads" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1803 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow file downloads" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1803 to REG_DWORD = 3.

Group ID (Vulid): V-6295
Group Title: DTBI120-Font download control - Restricted Sites
Rule ID: SV-16436r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI120
Rule Title: Allow font downloads for restricted sites zone is not disabled.

Vulnerability Discussion: Download of fonts can sometimes contain malicious code. Files should not be downloaded from restricted sites.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow font downloads" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1604 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow font downloads" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1604 to REG_DWORD = 3.

Group ID (Vulid): V-6297
Group Title: DTBI122-Access data sources - Restricted Sites
Rule ID: SV-16430r3_rule
Severity: CAT II

Rule Version (STIG-ID): DTBI122
Rule Title: Access data sources across domains restricted sites zones are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer can access data from another security zone using the Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO). If you enable this policy setting, users can load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you select Prompt in the drop-down box, users are queried to choose whether to allow a page to be loaded in the zone that uses MSXML or ADO to access data from another site in the zone. If you disable this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you do not configure this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Access data sources across domains" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1406 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Access data sources across domains" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1406 to REG_DWORD = 3.

Group ID (Vulid): V-6298
Group Title: DTBI123-Allow META REFRESH - Restricted Sites
Rule ID: SV-16463r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI123
Rule Title: Allow META REFRESH is not disabled.

Vulnerability Discussion: Allow META REFRESH must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow META REFRESH" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1608 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow META REFRESH" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1608 to REG_DWORD = 3.

Group ID (Vulid): V-6301
Group Title: DTBI126-Drag and drop or copy and paste - Restrict
Rule ID: SV-16434r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI126
Rule Title: Allow drag and drop or copy and paste files for restricted sites zone are not disabled.

Vulnerability Discussion: Drag and Drop of files must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow drag and drop or copy and paste files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1802 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow drag and drop or copy and paste files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1802 to REG_DWORD = 3.

Group ID (Vulid): V-6302

Group Title: DTBI127-Installation of desktop items - Restricted
Rule ID: SV-16438r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI127
Rule Title: Allow installation of desktop items for restricted sites zone is not disabled.

Vulnerability Discussion: Installation of items must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow installation of desktop items" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1800 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow installation of desktop items" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1800 to REG_DWORD = 3.

Group ID (Vulid): V-6303
Group Title: DTBI128-Launching programs and files in IFRAME-Res
Rule ID: SV-16450r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI128
Rule Title: Launching applications and files in an IFRAME is not disabled.

Vulnerability Discussion: Launching of programs in IFRAME must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Launching applications and files in an IFRAME" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1804 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Launching applications and files in an IFRAME" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1804 to REG_DWORD = 3.

Group ID (Vulid): V-6304
Group Title: DTBI129-Navigate sub-frames across domain - Restri
Rule ID: SV-16454r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI129
Rule Title: Navigate sub-frames across different domains for restricted sites zone are not disabled.

Vulnerability Discussion: Frames that navigate across different domains are a security concern because the user may think they are accessing pages on one site while they are actually accessing pages on another site.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Navigate sub-frames across different domains" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1607 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Navigate sub-frames across different domains" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1607 to REG_DWORD = 3.

Group ID (Vulid): V-6305
Group Title: DTBI130-Software channel permissions - Restricted
Rule ID: SV-16456r2_rule

Severity: CAT II
Rule Version (STIG-ID): DTBI130
Rule Title: Software channel permissions for restricted sites zone are not disabled.

Vulnerability Discussion: Software channel permissions must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Software channel permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1E05 is REG_DWORD = 65536 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Software channel permissions" will be set to “Enabled” and "High Safety" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1E05 to REG_DWORD = 65536 (decimal).

Group ID (Vulid): V-6307
Group Title: DTBI132-Userdata persistence - Restricted Sites
Rule ID: SV-16458r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI132
Rule Title: Userdata persistence for restricted sites zone is not disabled.

Vulnerability Discussion: No perseistant data should exist and be used in the Restricted sites zone.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Userdata persistence" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1606 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Userdata persistence" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1606 to REG_DWORD = 3.

Group ID (Vulid): V-6308
Group Title: DTBI133-Active scripting - Restricted Sites
Rule ID: SV-16461r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI133
Rule Title: Allow active scripting is not disabled.

Vulnerability Discussion: Active Scripting must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow active scripting" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1400 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow active scripting" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1400 to REG_DWORD = 3.

Group ID (Vulid): V-6309
Group Title: DTBI134-Allow paste operations via scripts-Restric
Rule ID: SV-16432r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI134
Rule Title: Allow cut, copy or paste operations from the clipboard via script are not disabled for restricted sites zone.

Vulnerability Discussion: The Allow paste operations via script must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1407 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow cut, copy or paste operations from the clipboard via script" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1407 to REG_DWORD = 3.

Group ID (Vulid): V-6311
Group Title: DTBI136-User Authentication - Logon - Restricted
Rule ID: SV-16452r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI136
Rule Title: Logon options for restricted sites zones are not enabled.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Logon options" will be set to “Enabled” and "Anonymous logon" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1A00 is REG_DWORD = 196608 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Logon options" will be set to “Enabled” and "Anonymous logon" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1A00 to REG_DWORD = 196608 (decimal).

Group ID (Vulid): V-6318
Group Title: DTBG010-DoD Root Certificate is not installed
Rule ID: SV-6388r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBG010
Rule Title: The DOD Root Certificate is not installed.

Vulnerability Discussion: The DOD root certificate will ensure that the trust chain is established for server certificate issued from the DOD CA.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedures: Open Internet Explorer. From the menu bar select Tools. From the Tools dropdown menu, select the Internet Options. From the Internet Options window, select the Content tab, from the Content tab window select the Publishers… button, from the Publisher window select the Trusted Root Certification Authorities Tab. Scroll through the Certificate Authorities list. Look for the DoD Class 3 Root CA. Click on DoD Class 3 Root CA. Select the View button. From the View Window select the Details Tab

Scroll to the bottom of the Window and select Thumbprint Algorithm in the bottom Pane you should see “sha1”, Next select Thumbprint

Criteria:
If there is no entry for the DoD Class 3 Root CA, then this is a Finding.

If the value of the Thumbprint Algorithm “sha1” and Thumbprint field is not: DoD Class 3 Root CA certificate is not:
10 f1 93 f3 40 ac 91 d6 de 5f 1e dc 00 62 47 c4 f2 5d 96 71,
then this is a Finding.

Check Content:
Procedure: Use the Tools/Options/Advanced/Encryption dialog. On the Select the View Certificates button. On the Certificate Manager window, select the Authorities tab. Scroll through the Certificate Name list to the U.S. Government heading. Look for the entry for the DoD Class 3 Root CA.
If there is an entry for the DoD Class 3 Root CA, select the entry and then the View button. On the Certificate Viewer window, determine the value of the MD5 Fingerprint field.

Criteria:
If there is no entry for the DoD Class 3 Root CA, then this is a Finding.

If the value of the MD5 Fingerprint field of the DoD Class 3 Root CA certificate is not:
8C:48:08:65:BB:DA:FF:9F:FD:8C:E2:95:E0:96:B9:9D,
then this is a Finding.

If the value of the SHA1 Fingerprint field of the DoD Class 3 Root CA certificate is not:

10:F1:93:F3:40:AC:91:D6:DE:5F:1E:DC:00:62:47:C4:F2:5D:96:71,then this is a Finding.

Fix Text: Install the DOD root certificate.

Group ID (Vulid): V-7007
Group Title: DTBI121-Java Permissions not set for Restricted
Rule ID: SV-16448r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI121
Rule Title: Java permissions for restricted sites zone are not disabled.

Vulnerability Discussion: Java must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-14245
Group Title: DTBI697 - IE - Users enable or disable add-ons
Rule ID: SV-14856r5_rule
Severity: CAT III
Rule Version (STIG-ID): DTBI697
Rule Title: Internet Explorer - Do not allow users to enable or disable add-ons.

Vulnerability Discussion: This check verifies that the system is configured to allow users to enable or disable add-ons through Add-On Manager in Internet Explorer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet

Explorer “Do Not Allow Users to enable or Disable Add-Ons” will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions

Criteria: If the value NoExtensionManagement “does not” exist or the value is set to REG_DWORD = 0, this is not a finding.

If the value NoExtensionManagement “does” exist and is set to REG_DWORD = 1 (decimal), this is a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Do Not Allow Users to enable or Disable Add-Ons” will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions

Criteria: Remove the value NoExtensionManagement or set to REG_DWORD = 0 (decimal).

Group ID (Vulid): V-15490
Group Title: DTBI305-Automatic configuration is not disabled
Rule ID: SV-16337r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI305
Rule Title: Automatic configuration of Internet Explorer is not disabled.

Vulnerability Discussion: This setting specifies to automatically detect the proxy server settings used to connect to the Internet and customize Internet Explorer. This setting specifies that Internet explorer use the configuration settings provided in a file by the system administrator. If you enable this policy setting, the user will not be able to do automatic configuration. You can import your current connection settings from your machine using Internet Explorer Maintenance under Admin Templates using group policy editor. If you disable or do no configure this policy setting, the user will have the freedom to automatically configure these settings.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable changing Automatic Configuration settings" will be
set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: If the value Autoconfig is REG_DWORD = 1 (Hex), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable changing Automatic Configuration settings" will be
set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: Set the value Autoconfig to REG_DWORD = 1 (Hex).

Group ID (Vulid): V-15491
Group Title: DTBI310-Showing the splash screen is not disabled
Rule ID: SV-16338r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI310
Rule Title: Showing the splash screen is not disabled.

Vulnerability Discussion: The Disable showing the splash screen setting prevents the Internet Explorer splash screen from appearing when users start the browser. Enabling this policy causes the splash screen, which normally displays the program name, licensing, and copyright information, to not display. Setting Disable showing the splash screen to disable or Not Configured allows the splash screen to display when users start the browser.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable showing the splash screen" will be
set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions

Criteria: If the value NoSplash is REG_DWORD = 1 (Hex), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable showing the splash screen" will be
set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Infodelivery\Restrictions

Criteria: Set the value NoSplash to REG_DWORD = 1 (Hex).

Group ID (Vulid): V-15492
Group Title: DTBI315 - Prevent participation in the Customer Ex
Rule ID: SV-16339r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI315
Rule Title: Prevent participation in the Customer Experience Improvement Program is not disabled.

Vulnerability Discussion: This setting controls whether users can participate in the Microsoft Customer Experience Improvement Program to help improve Microsoft applications.

When users choose to participate in the Customer Experience Improvement Program (CEIP), applications automatically send information to Microsoft about how the applications are used. This information is combined with other CEIP data to help Microsoft solve problems and to improve the products and features customers use most often. This feature does not collect users' names, addresses, or any other identifying information except the IP address that is used to send the data.
By default, users have the opportunity to opt into participation in the CEIP the first time they run an application. If your organization has policies that govern the use of external resources such as the CEIP, allowing users to opt in to the program might cause them to violate these policies.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent participation in the Customer Experience Improvement Program" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\SQM

Criteria: If the value DisableCustomerImprovementProgram is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent participation in the Customer Experience Improvement Program" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\SQM

Criteria: Set the value DisableCustomerImprovementProgram to REG_DWORD = 0.

Group ID (Vulid): V-15494
Group Title: DTBI325 - Turn off the Security Settings Check fea
Rule ID: SV-16341r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI325
Rule Title: Turn off the Security Settings Check feature is not disabled.

Vulnerability Discussion: This policy setting turns off the Security Settings Check feature, which checks Internet Explorer security settings to determine when the settings put Internet Explorer at risk. If you enable this policy setting, the security settings check will not be performed. If you disable or do not configure this policy setting, the security settings check will be performed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off the Security Settings Check feature" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Security

Criteria: If the value DisableSecuritySettingsCheck is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off the Security Settings Check feature" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Security

Criteria: Set the value DisableSecuritySettingsCheck to REG_DWORD = 0.

Group ID (Vulid): V-15495
Group Title: DTBI330 - Turn off Managing Phishing filter is not
Rule ID: SV-16342r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI330
Rule Title: Turn off Managing Phishing filter is not disabled.

Vulnerability Discussion: This policy setting allows the user to enable a phishing filter that will warn if the Web site being visited is known for fraudulent attempts to gather personal information through "phishing." If you enable this policy setting, the user will not be prompted to enable the phishing filter. You must specify which mode the phishing filter uses: manual, automatic, or off. If you select manual mode, the phishing filter performs only local analysis and users are prompted to permit any data to be sent to Microsoft. If the feature is fully enabled, all website addresses not contained on the filter's whitelist will be sent automatically to Microsoft without prompting the user. If you disable or do not configure this policy setting, the user will be prompted to decide the mode of operation for the phishing filter.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Managing Phishing filter" will be set to “Enabled” and "Off" selected.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\PhishingFilter

Criteria: If the value Enabled is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Managing Phishing filter" will be set to “Enabled” and "Off" selected.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\PhishingFilter

Criteria: Set the value Enabled to REG_DWORD = 0.

Group ID (Vulid): V-15497
Group Title: DTBI340 - Allow active content from CDs to run on
Rule ID: SV-16344r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI340
Rule Title: Allow active content from CDs to run on user machines is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether users receive a dialog requesting permission for active content on a CD to run. If you enable this policy setting, active content on a CD will run without a prompt.
If you disable this policy setting, active content on a CD will always prompt before running. If you do not configure this policy, users can choose whether to be prompted before running active content on a CD.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow active content from CDs to run on user machines" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\Settings

Criteria: If the value LOCALMACHINE_CD_UNLOCK is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow active content from CDs to run on user machines" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LOCALMACHINE_LOCKDOWN\Settings

Criteria: Set the value LOCALMACHINE_CD_UNLOCK to REG_DWORD = 0.

Group ID (Vulid): V-15499
Group Title: DTBI350 - Allow software to run or install even if
Rule ID: SV-16346r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI350
Rule Title: Allow software to run or install even if the signature is invalid is not disabled.

Vulnerability Discussion: Microsoft ActiveX controls and file downloads often have digital signatures attached that vouch for both the file's integrity and the identity of the signer (creator) of the software. Such signatures help ensure that unmodified.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow software to run or install even if the signature is invalid" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Download

Criteria: If the value RunInvalidSignatures is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow software to run or install even if the signature is invalid" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Download

Criteria: Set the value RunInvalidSignatures to REG_DWORD = 0.

Group ID (Vulid): V-15500
Group Title: DTBI355 - Allow third-party browser extensions are
Rule ID: SV-16347r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI355
Rule Title: Allow third-party browser extensions are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer will launch COM add-ons known as browser helper objects, such as toolbars. Browser helper objects may contain flaws such as buffer overruns which impact Internet Explorer's performance or stability. If you enable this policy setting, Internet Explorer automatically launches any browser helper objects that are installed on the user's computer. If you disable this policy setting, browser helper objects do not launch. If you do not configure this policy, Internet Explorer automatically launches any browser helper objects that are installed on the user's computer.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow third-party browser extensions" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: If the value Enable Browser Extensions is REG_SZ = no, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Allow third-party browser extensions" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Set the value Enable Browser Extensions to REG_SZ = no.

Group ID (Vulid): V-15501
Group Title: DTBI360 - Automatically check for Internet Explore
Rule ID: SV-16348r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI360
Rule Title: Automatically check for Internet Explorer updates are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer checks the Internet for newer versions. When Internet Explorer is set to do this, the checks occur approximately every 30 days, and users are prompted to install new versions as they become available. If you enable this policy setting, Internet Explorer checks the Internet for a new version approximately every 30 days and prompts the user to download new versions when they are available. If you disable this policy setting, Internet Explorer does not check the Internet for new versions of the browser, so does not prompt users to install them. If you do not configure this policy setting, Internet Explorer does not check the Internet for new versions of the browser, so does not prompt users to install them.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Automatically check for Internet Explorer updates" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: If the value NoUpdateCheck is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Automatically check for Internet Explorer updates" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Set the value NoUpdateCheck to REG_DWORD = 1.

Group ID (Vulid): V-15502
Group Title: DTBI365 - Check for server certificate revocation
Rule ID: SV-16349r3_rule

Severity: CAT II
Rule Version (STIG-ID): DTBI365
Rule Title: Check for server certificate revocation is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer will check revocation status of servers' certificates. Certificates are revoked when they have been compromised or are no longer valid, and this option protects users from submitting confidential data to a site that may be fraudulent or not secure. If you enable this policy setting, Internet Explorer will check to see if server certificates have been revoked. If you disable this policy setting, Internet Explorer will not check server certificates to see if they have been revoked. If you do not configure this policy setting, Internet Explorer will not check server certificates to see if they have been revoked.

Responsibility: System Administrator
IAControls: IATS-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for server certificate revocation" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings

Criteria: If the value CertificateRevocation is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for server certificate revocation" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings

Criteria: Set the value CertificateRevocation to REG_DWORD = 1.

Group ID (Vulid): V-15503
Group Title: DTBI370 - Check for signatures on downloaded progr
Rule ID: SV-16350r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI370
Rule Title: Check for signatures on downloaded programs is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether Internet Explorer checks for digital signatures (which identifies the publisher of signed software and verifies it hasn't been modified or tampered with) on user computers before downloading executable programs. If you enable this policy setting, Internet Explorer will check the digital signatures of executable programs and display their identities before downloading them to user computers.
If you disable this policy setting, Internet Explorer will not check the digital signatures of executable programs or display their identities before downloading them to user computers. If you do not configure this policy, Internet Explorer will not check the digital signatures of executable programs or display their identities before downloading them to user computers.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for signatures on downloaded programs" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Download

Criteria: If the value CheckExeSignatures is REG_SZ = yes, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Advanced Page -> "Check for signatures on downloaded programs" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Download

Criteria: Set the value CheckExeSignatures to REG_SZ = yes.

Group ID (Vulid): V-15504
Group Title: DTBI375 - Intranet Sites: Include all network path
Rule ID: SV-16351r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI375
Rule Title: Intranet Sites: Include all network paths (UNCs) are disabled.

Vulnerability Discussion: This policy setting controls whether URLs representing UNCs are mapped into the local Intranet security zone. If you enable this policy setting, all network paths are mapped into the Intranet Zone. If you disable this policy setting, network paths are not necessarily mapped into the Intranet Zone (other rules might map one there). If you do not configure this policy setting, users choose whether network paths are mapped into the Intranet Zone.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> "Intranet Sites: Include all network paths (UNCs)" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Criteria: If the value UNCAsIntranet is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> "Intranet Sites: Include all network paths (UNCs)" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Criteria: Set the value UNCAsIntranet to REG_DWORD = 0.

Group ID (Vulid): V-15507
Group Title: DTBI385 - Allow script-initiated windows without s
Rule ID: SV-16354r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI385
Rule Title: Allow script-initiated windows without size or position constraints for internet zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars.
If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow script-initiated windows without size or position constraints" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 2102 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow script-initiated windows without size or position constraints" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 2102 to REG_DWORD = 3.

Group ID (Vulid): V-15508
Group Title: DTBI390 - Allow script-initiated windows without s
Rule ID: SV-16355r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI390
Rule Title: Allow script-initiated windows without size or position constraints for restricted sites zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars.
If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow script-initiated windows without size or position constraints" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2102 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow script-initiated windows without size or position constraints" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2102 to REG_DWORD = 3.

Group ID (Vulid): V-15509
Group Title: DTBI395 - Allow Scriptlets are not disabled.
Rule ID: SV-16356r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI395
Rule Title: Allow Scriptlets are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether scriptlets can be allowed.

If you enable this policy setting, users will be able to run scriptlets.
If you disable this policy setting, users will not be able to run scriptlets.
If you do not configure this policy setting, a scriptlet can be enabled or disabled by the user.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow Scriptlets" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1209 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Allow Scriptlets" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1209 to REG_DWORD = 3.

Group ID (Vulid): V-15513
Group Title: DTBI415 - Automatic prompting for file downloads i
Rule ID: SV-16360r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI415
Rule Title: Automatic prompting for file downloads is not enabled.

Vulnerability Discussion: This policy setting determines whether users will be prompted for non user-initiated file downloads. Regardless of this setting, users will receive file download dialogs for user-initiated downloads. If you enable this setting, users will receive a file download dialog for automatic download attempts.
If you disable or do not configure this setting, file downloads that are not user-initiated will be blocked, and users will see the Information Bar instead of the file download dialog. Users can then click the Information Bar to allow the file download prompt.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Automatic prompting for file downloads" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 2200 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Automatic prompting for file downloads" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 2200 to REG_DWORD = 0.

Group ID (Vulid): V-15515
Group Title: DTBI425 - Java permissions for my computer are not
Rule ID: SV-16362r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI425
Rule Title: Java permissions for my computer are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.
If you enable this policy setting, you can choose options from the drop-down box. Custom, to control permissions settings individually. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.
If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.
Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Local Machine Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Local Machine Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15516
Group Title: DTBI430 - Java permissions for my computer group p
Rule ID: SV-16363r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI430
Rule Title: Java permissions for my computer group policy are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.
If you enable this policy setting, you can choose options from the drop-down box. Custom, to control permissions settings individually. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.
If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.
Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Local Machine Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Local Machine Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15517
Group Title: DTBI435 - Java permissions for group policy for lo
Rule ID: SV-16364r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI435
Rule Title: Java permissions for group policy for local intranet zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.
If you enable this policy setting, you can choose options from the drop-down box. Custom, to control permissions

settings individually. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.
If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.
Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Intranet Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Intranet Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15518
Group Title: DTBI440 - Java permissions for group policy for tr
Rule ID: SV-16365r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI440
Rule Title: Java permissions for group policy for trusted sites zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.
If you enable this policy setting, you can choose options from the drop-down box. Custom, to control permissions settings individually. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.
If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.
Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Trusted Sites Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Trusted Sites Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15519
Group Title: DTBI445 - Java permissions for group policy for in
Rule ID: SV-16366r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI445
Rule Title: Java permissions for group policy for internet zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.
If you enable this policy setting, you can choose options from the drop-down box. Custom, to control permissions settings individually. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.
If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.
Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15520
Group Title: DTBI450 - Java permissions for group policy for re
Rule ID: SV-16367r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI450
Rule Title: Java permissions for group policy for restricted sites zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage permissions for Java applets.
If you enable this policy setting, you can choose options from the drop-down box. Custom, to control permissions settings individually. Low Safety enables applets to perform all operations. Medium Safety enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. High Safety enables applets to run in their sandbox. Disable Java to prevent any applets from running.
If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to High Safety.
Note: This only applies to MS Java, not Sun Java.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Restricted Sites Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4

Criteria: If the value 1C00 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Restricted Sites Zone -> "Java permissions" will be set to “Enabled” and "Disable Java" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following keys:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4

Criteria: Set the value 1C00 to REG_DWORD = 0.

Group ID (Vulid): V-15521

Group Title: DTBI455 - Loose or un-compiled XAML files for inte
Rule ID: SV-16368r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI455
Rule Title: Loose or un-compiled XAML files for internet zone are not disabled.

Vulnerability Discussion: These are eXtensible Application Markup Language (XAML) files. XAML is an XML-based declarative markup language commonly used for creating rich user interfaces and graphics that leverage the Windows Presentation Foundation. If you enable this policy setting and the dropdown box is set to Enable, .XAML files will be automatically loaded inside Internet Explorer 7.0. User will not be able to change this behavior. If the dropdown box is set to Prompt, users will receive a prompt for loading .XAML files. If you disable this policy setting, .XAML files will not be loaded inside Internet Explorer 7. User will not be able to change this behavior. If you do not configure this policy setting, users will have the freedom to decide whether to load XAML files inside Internet Explorer 7.0.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Loose or un-compiled XAML files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 2402 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Loose or un-compiled XAML files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 2402 to REG_DWORD = 3.

Group ID (Vulid): V-15522
Group Title: DTBI460 - Loose or un-compiled XAML files for rest
Rule ID: SV-16369r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI460
Rule Title: Loose or un-compiled XAML files for restricted sites zone are not disabled.

Vulnerability Discussion: These are eXtensible Application Markup Language (XAML) files. XAML is an XML-based declarative markup language commonly used for creating rich user interfaces and graphics that leverage the Windows Presentation Foundation. If you enable this policy setting and the dropdown box is set to Enable, .XAML files will be automatically loaded inside Internet Explorer 7.0. User will not be able to change this behavior. If the dropdown box is set to Prompt, users will receive a prompt for loading .XAML files. If you disable this policy setting, .XAML files will not be loaded inside Internet Explorer 7. User will not be able to change this behavior. If you do not configure this policy setting, users will have the freedom to decide whether to load XAML files inside Internet Explorer 7.0.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Loose or un-compiled XAML files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2402 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Loose or un-compiled XAML files" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2402 to REG_DWORD = 3.

Group ID (Vulid): V-15523
Group Title: DTBI465 - Open files based on content, not file ex
Rule ID: SV-16370r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI465
Rule Title: Open files based on content, not file extension for internet zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage MIME sniffing for file promotion from one type to another based on a MIME sniff. A MIME sniff is the recognition by Internet Explorer of the file type based on a bit signature. If you enable this policy setting, the MIME Sniffing Safety Feature will not apply in this zone. The security zone will run without the added layer of security provided by this feature. If you disable this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this zone, as dictated by the feature control setting for the process.
If you do not configure this policy setting, the MIME Sniffing Safety Feature will not apply in this zone.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Open files based on content, not file extension" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 2100 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Open files based on content, not file extension" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 2100 to REG_DWORD = 3.

Group ID (Vulid): V-15524
Group Title: DTBI470 - Open files based on content, not file ex
Rule ID: SV-16371r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI470
Rule Title: Open files based on content, not file extension for restricted sites zone are not disabled.

Vulnerability Discussion: This policy setting allows you to manage MIME sniffing for file promotion from one type to another based on a MIME sniff. A MIME sniff is the recognition by Internet Explorer of the file type based on a bit signature. If you enable this policy setting, the MIME Sniffing Safety Feature will not apply in this zone. The security zone will run without the added layer of security provided by this feature. If you disable this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this zone, as dictated by the feature control setting for the process.
If you do not configure this policy setting, the MIME Sniffing Safety Feature will not apply in this zone.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Open files based on content, not file extension" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2100 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Open files based on content, not file extension" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2100 to REG_DWORD = 3.

Group ID (Vulid): V-15525

Group Title: DTBI475 - Turn Off First-Run Opt-In for internet z
Rule ID: SV-16372r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI475
Rule Title: Turn Off First-Run Opt-In for internet zone is not disabled.

Vulnerability Discussion: This policy setting controls the First Run response that users see on a zone by zone basis. When a user encounters a new control that has not previously run in Internet Explorer, they may be prompted to approve the control. This feature determines if the user gets the prompt or not.
If you enable this policy setting, the Gold Bar prompt will be turned off in the corresponding zone. If you disable this policy setting, the Gold Bar prompt will be turned on in the corresponding zone. If you do not configure this policy setting, the first-run prompt is turned off by default.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn Off First-Run Opt-In" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1208 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn Off First-Run Opt-In" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1208 to REG_DWORD = 0.

Group ID (Vulid): V-15526
Group Title: DTBI480 - Turn Off First-Run Opt-In for restricted
Rule ID: SV-16373r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI480
Rule Title: Turn Off First-Run Opt-In for restricted sites zone are not disabled.

Vulnerability Discussion: This policy setting controls the First Run response that users see on a zone by zone basis. When a user encounters a new control that has not previously run in Internet Explorer, they may be prompted to approve the control. This feature determines if the user gets the prompt or not.
If you enable this policy setting, the Gold Bar prompt will be turned off in the corresponding zone. If you disable this policy setting, the Gold Bar prompt will be turned on in the corresponding zone. If you do not configure this policy setting, the first-run prompt is turned off by default.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn Off First-Run Opt-In" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1208 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn Off First-Run Opt-In" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1208 to REG_DWORD = 0.

Group ID (Vulid): V-15527
Group Title: DTBI485 - Turn on Protected Mode internet zone is
Rule ID: SV-16374r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI485
Rule Title: Turn on Protected Mode internet zone is not enabled.

Vulnerability Discussion: Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system. If you enable this policy setting, Protected Mode will be turned on. Users will not be able to turn off protected mode. If you disable this policy setting, Protected Mode will be turned off. It will revert to Internet Explorer 6 behavior that allows for Internet Explorer to write to the registry and the file system. Users will not be able to turn on protected mode. If you do not configure this policy, users will be able to turn on or off protected mode.
Requires Windows Vista; will be ignored by Windows XP.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn on Protected Mode" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 2500 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Turn on Protected Mode" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 2500 to REG_DWORD = 0.

Group ID (Vulid): V-15528
Group Title: DTBI490 - Turn on Protected Mode for restricted si
Rule ID: SV-16375r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI490
Rule Title: Turn on Protected Mode for restricted sites zone is not enabled.

Vulnerability Discussion: VISTA Only
Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system. If you enable this policy setting, Protected Mode will be turned on. Users will not be able to turn off protected mode. If you disable this policy setting, Protected Mode will be turned off. It will revert to Internet Explorer 6 behavior that allows for Internet Explorer to write to the registry and the file system. Users will not be able to turn on protected mode. If you do not configure this policy, users will be able to turn on or off protected mode.
Requires Windows Vista; will be ignored by Windows XP.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn on Protected Mode" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2500 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Turn on Protected Mode" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2500 to REG_DWORD = 0.

Group ID (Vulid): V-15529
Group Title: DTBI495 - Use Pop-up Blocker for internet zone is
Rule ID: SV-16376r3_rule

Severity: CAT II
Rule Version (STIG-ID): DTBI495
Rule Title: Use Pop-up Blocker for internet zone is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether unwanted pop-up windows appear. Pop-up windows that are opened when the end user clicks a link are not blocked. If you enable this policy setting, most unwanted pop-up windows are prevented from appearing. If you disable this policy setting, pop-up windows are not prevented from appearing. If you do not configure this policy setting, most unwanted pop-up windows are prevented from appearing.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Use Pop-up Blocker" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1809 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Use Pop-up Blocker" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1809 to REG_DWORD = 0.

Group ID (Vulid): V-15530
Group Title: DTBI500 - Use Pop-up Blocker for restricted sites
Rule ID: SV-16377r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI500
Rule Title: Use Pop-up Blocker for restricted sites zone is not enabled.

Vulnerability Discussion: This policy setting allows you to manage whether unwanted pop-up windows appear. Pop-up windows that are opened when the end user clicks a link are not blocked. If you enable this policy setting, most unwanted pop-up windows are prevented from appearing. If you disable this policy setting, pop-up windows are not prevented from appearing. If you do not configure this policy setting, most unwanted pop-up windows are prevented from appearing.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Use Pop-up Blocker" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1809 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Use Pop-up Blocker" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1809 to REG_DWORD = 0.

Group ID (Vulid): V-15533
Group Title: DTBI515 - Web sites in less privileged Web content
Rule ID: SV-16380r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI515
Rule Title: Web sites in less privileged Web content zones can navigate into internet zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Web sites from less privileged zones, such as Restricted Sites, can navigate into this zone.
If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Web sites in less privileged Web content zones can navigate into this zone" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 2101 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Internet Zone -> "Web sites in less privileged Web content zones can navigate into this zone" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria:Set the value 2101 to REG_DWORD = 3.

Group ID (Vulid): V-15534
Group Title: DTBI520 - Web sites in less privileged Web content
Rule ID: SV-16381r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI520
Rule Title: Web sites in less privileged Web content zones can navigate into restricted sites zone is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether Web sites from less privileged zones, such as Restricted Sites, can navigate into this zone.
If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Web sites in less privileged Web content zones can navigate into this zone" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2101 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Web sites in less privileged Web content zones can navigate into this zone" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2101 to REG_DWORD = 3.

Group ID (Vulid): V-15545
Group Title: DTBI575 - Allow binary and script behaviors are no
Rule ID: SV-16392r3_rule
Severity: CAT II

Rule Version (STIG-ID): DTBI575
Rule Title: Allow binary and script behaviors are not disabled.

Vulnerability Discussion: This policy setting allows you to manage dynamic binary and script behaviors: components that encapsulate specific functionality for HTML elements to which they were attached. If you enable this policy setting, binary and script behaviors are available. If you select Administrator approved in the drop-down box, only behaviors listed in the Admin-approved Behaviors under Binary Behaviors Security Restriction policy are available. If you disable this policy setting, binary and script behaviors are not available unless applications have implemented a custom security manager. If you do not configure this policy setting, binary and script behaviors are available.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow binary and script behaviors" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2000 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Allow binary and script behaviors" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2000 to REG_DWORD = 3.

Group ID (Vulid): V-15546
Group Title: DTBI580 - Automatic prompting for file downloads i
Rule ID: SV-16393r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI580
Rule Title: Automatic prompting for file downloads is not enabled.

Vulnerability Discussion: This policy setting determines whether users will be prompted for non user-initiated file downloads. Regardless of this setting, users will receive file download dialogs for user-initiated downloads. If you enable this setting, users will receive a file download dialog for automatic download attempts. If you disable or do not configure this setting, file downloads that are not user-initiated will be blocked, and users will see the Information Bar instead of the file download dialog. Users can then click the Information Bar to allow the file download prompt.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Automatic prompting for file

downloads" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2200 is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Automatic prompting for file downloads" will be set to “Enabled” and "Enable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2200 to REG_DWORD = 0.

Group ID (Vulid): V-15548
Group Title: DTBI590 - Internet Explorer Processes for MIME han
Rule ID: SV-16395r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI590
Rule Title: Internet Explorer Processes for MIME handling is not enabled. (Reserved)

Vulnerability Discussion: Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. The Consistent MIME Handling\Internet Explorer Processes policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data provided by the file. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistent and properly labeled helps prevent malicious file downloads from infecting your network. Therefore, this appendix recommends you configure this policy as Enabled for all environments specified in this guide.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-15549
Group Title: DTBI595 - Internet Explorer Processes for MIME sni
Rule ID: SV-16396r4_rule
Severity: CAT III
Rule Version (STIG-ID): DTBI595
Rule Title: Internet Explorer Processes for MIME sniffing is not enabled. (Reserved)

Vulnerability Discussion: MIME sniffing is the process of examining the content of a MIME file to determine its context — whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When set to Enabled, MIME sniffing will never promote a file of one type to a more dangerous file type. Disabling MIME sniffing configures Internet Explorer processes to allow a MIME sniff that promotes a file of one type to a more dangerous file type. For example, promoting a text file to an executable file is a dangerous promotion because any code in the supposed text file would be executed. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistently handled helps prevent malicious file downloads from infecting your network. Therefore, this appendix recommends you configure this policy as Enabled for all environments specified in this guide. Note: This setting works in conjunction with, but does not replace, the Consistent MIME Handling settings.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-15550
Group Title: DTBI600 - Internet Explorer Processes for MK proto
Rule ID: SV-16397r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI600
Rule Title: Internet Explorer Processes for MK protocol is not enabled. (Explorer)

Vulnerability Discussion: The MK Protocol Security Restriction policy setting reduces attack surface area by blocking the seldom used MK protocol. Some older Web applications use the MK protocol to retrieve information from compressed files. Setting this policy to Enabled blocks the MK protocol for Windows Explorer and Internet Explorer, which causes resources that use the MK protocol to fail. Disabling this setting allows applications to use the MK protocol API. Because the MK protocol is not widely used, it should be blocked wherever it is not needed. This appendix recommends you configure this setting to Enabled to block the MK protocol unless you specifically need it in your environment. Note: Because resources that use the MK protocol will fail when you deploy this setting, you should ensure that none of your applications use the MK protocol.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL

Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL

Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15551
Group Title: DTBI605 - Internet Explorer Processes for MK proto
Rule ID: SV-16398r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI605
Rule Title: Internet Explorer Processes for MK protocol is not enabled. (IExplore)

Vulnerability Discussion: The MK Protocol Security Restriction policy setting reduces attack surface area by blocking the seldom used MK protocol. Some older Web applications use the MK protocol to retrieve information from compressed files. Setting this policy to Enabled blocks the MK protocol for Windows Explorer and Internet Explorer, which causes resources that use the MK protocol to fail. Disabling this setting allows applications to use the MK protocol API. Because the MK protocol is not widely used, it should be blocked wherever it is not needed. This appendix recommends you configure this setting to Enabled to block the MK protocol unless you specifically need it in your environment. Note: Because resources that use the MK protocol will fail when you deploy this setting, you should ensure that none of your applications use the MK protocol.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to "Enabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15552
Group Title: DTBI610 - Internet Explorer Processes for Zone Ele
Rule ID: SV-16399r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI610
Rule Title: Internet Explorer Processes for Zone Elevation is not enabled. (Reserved)

Vulnerability Discussion: Internet Explorer places restrictions on each Web page it opens that are dependent upon the location of the Web page (such as Internet zone, Intranet zone, or Local Machine zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine zone, which makes the Local Machine security zone a prime target for malicious attackers. If you enable this policy setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach stops content running in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes. Because of the severity and relative frequency of zone elevation attacks, this appendix recommends that you configure this setting as Enabled in all environments.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-15556
Group Title: DTBI630 - Internet Explorer Processes for Download
Rule ID: SV-16403r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI630
Rule Title: Internet Explorer Processes for Download prompt is not enabled. (Reserved)

Vulnerability Discussion: In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users' hard drives if they click the wrong button and accept the download. If you configure the Restrict File Download\Internet Explorer Processes policy setting to Enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting as Disabled, prompting will occur for file downloads that are not user-initiated for Internet Explorer processes. Note: This setting is configured as Enabled in all environments specified in this guide to help prevent attackers from placing arbitrary code on users' computers.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD

Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD

Criteria: Set the value (Reserved) to REG_SZ = 1.

Group ID (Vulid): V-15557
Group Title: DTBI635 - Internet Explorer Processes for Download
Rule ID: SV-16404r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI635
Rule Title: Internet Explorer Processes for Download prompt is not enabled. Explorer

Vulnerability Discussion: In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users' hard drives if they click the wrong button and accept the download. If you configure the Restrict File Download\Internet Explorer Processes policy setting to Enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting as Disabled, prompting will occur for file downloads that are not user-initiated for Internet Explorer processes. Note: This setting is configured as Enabled in all environments specified in this guide to help prevent attackers from placing arbitrary code on users' computers.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD

Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD

Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15558
Group Title: DTBI640 - Internet Explorer Processes for Download
Rule ID: SV-16405r4_rule
Severity: CAT II

Rule Version (STIG-ID): DTBI640
Rule Title: Internet Explorer Processes for Download prompt is not enabled. IExplore

Vulnerability Discussion: In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on users' hard drives if they click the wrong button and accept the download. If you configure the Restrict File Download\Internet Explorer Processes policy setting to Enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting as Disabled, prompting will occur for file downloads that are not user-initiated for Internet Explorer processes. Note: This setting is configured as Enabled in all environments specified in this guide to help prevent attackers from placing arbitrary code on users' computers.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Restrict File Download -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_FILEDOWNLOAD

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15559
Group Title: DTBI645 - Internet Explorer Processes for restrict
Rule ID: SV-16406r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI645
Rule Title: Internet Explorer Processes for restricting pop-up windows is not enabled. (Reserved)

Vulnerability Discussion: Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. Often, disreputable Web sites will resize windows to either hide other windows or force you to interact with a window that contains malicious code. The Scripted Window Security Restrictions security feature restricts pop-up windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or hide other windows’ title and status bars. If you enable the Scripted Window Security Restrictions\Internet Explorer Processes policy setting, pop-up windows and other restrictions apply for Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts can continue to create pop-up windows and windows that hide other windows. This appendix recommends you configure this setting to Enabled to help prevent malicious Web sites from controlling your Internet Explorer windows or fooling users into clicking on the wrong window.

Responsibility: System Administrator

IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

Criteria: If the value (Reserved) is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

Criteria: Set the value (Reserved) is REG_SZ = 1.

Group ID (Vulid): V-15560
Group Title: DTBI650 - Run .NET Framework-reliant components no
Rule ID: SV-16407r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI650
Rule Title: Run .NET Framework-reliant components not signed with Authenticode are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether .NET Framework components that are signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.
If you enable this policy setting, Internet Explorer will execute signed managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute signed managed components. If you disable this policy setting, Internet Explorer will not execute signed managed components. If you do not configure this policy setting, Internet Explorer will execute signed managed components.

This policy setting allows you to manage whether .NET Framework components that are not signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.
If you enable this policy setting, Internet Explorer will execute unsigned managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute unsigned managed components. If you disable this policy setting, Internet Explorer will not execute unsigned managed components. If you do not configure this policy setting, Internet Explorer will execute unsigned managed components.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant

components not signed with Authenticode" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2004 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant components not signed with Authenticode" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2004 to REG_DWORD = 3.

Group ID (Vulid): V-15561
Group Title: DTBI655 - Run .NET Framework-reliant components si
Rule ID: SV-16408r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI655
Rule Title: Run .NET Framework-reliant components signed with Authenticode are not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether .NET Framework components that are not signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link.
If you enable this policy setting, Internet Explorer will execute unsigned managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute unsigned managed components. If you disable this policy setting, Internet Explorer will not execute unsigned managed components. If you do not configure this policy setting, Internet Explorer will execute unsigned managed components.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant components signed with Authenticode" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 2001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Run .NET Framework-reliant components signed with Authenticode" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 2001 to REG_DWORD = 3.

Group ID (Vulid): V-15562
Group Title: DTBI670 - Scripting of Java applets is not disable
Rule ID: SV-16409r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI670
Rule Title: Scripting of Java applets is not disabled.

Vulnerability Discussion: This policy setting allows you to manage whether applets are exposed to scripts within the zone. If you enable this policy setting, scripts can access applets automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow scripts to access applets. If you disable this policy setting, scripts are prevented from accessing applets. If you do not configure this policy setting, scripts can access applets automatically without user intervention.
Note: this only applies to MS Java, not to Sun Java.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Scripting of Java applets" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1402 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Restricted Sites Zone -> "Scripting of Java applets" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: Set the value 1402 to REG_DWORD = 3.

Group ID (Vulid): V-15563
Group Title: DTBI675 - Turn off changing the URL to be displaye
Rule ID: SV-16410r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI675
Rule Title: Turn off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools

is not disabled.

Vulnerability Discussion: This policy setting allows checking for updates for Internet Explorer from the specified URL, included by default in Internet Explorer. If you enable this policy setting, users will not be able to change the URL to be displayed for checking updates to Internet Explorer and Internet Tools. You must specify the URL to be displayed for checking updates to Internet Explorer and Internet Tools. If you disable or do not configure this policy setting, users will be able to change the URL to be displayed for checking updates to Internet Explorer and Internet Tools.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools" will be set to “Enabled” and "blank or empty" selection box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: The Update_Check_Page value must exist. The value must contain no data value. If the value Update_Check_Page is not present this is a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off changing the URL to be displayed for checking updates to Internet Explorer and Internet Tools" will be set to “Enabled” and "blank or empty" selection box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Create the value Update_Check_Page .
The value must contain no data.

Group ID (Vulid): V-15564
Group Title: DTBI680 - Turn off configuring the update check in
Rule ID: SV-16411r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI680
Rule Title: Turn off configuring the update check interval is not disabled.

Vulnerability Discussion: This setting specifies the update check interval. The default value is 30 days.
If you enable this policy setting, the user will not be able to configure the update check interval. You have to specify the update check interval.
If you disable or do not configure this policy setting, the user will have the freedom to configure the update check interval.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off configuring the update check interval (in days)" will be set to “Enabled” and "30" selected from drop down box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: If the value Update_Check_Interval is REG_DWORD = 30 (Decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Component Updates -> Periodic check for updates to Internet Explorer and Internet Tools -> "Turn off configuring the update check interval (in days)" will be set to “Enabled” and "30" selected from drop down box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Set the value Update_Check_Interval to REG_DWORD = 30 (Decimal).

Group ID (Vulid): V-15565
Group Title: DTBI592 - Internet Explorer Processes for MIME han
Rule ID: SV-16412r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI592
Rule Title: Internet Explorer Processes for MIME handling is not enabled. Explorer

Vulnerability Discussion: Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. The Consistent MIME Handling\Internet Explorer Processes policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data provided by the file. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistent and properly labeled helps prevent malicious file downloads from infecting your network. Therefore, this appendix recommends you configure this policy as Enabled for all environments specified in this guide.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15566
Group Title: DTBI594 - Internet Explorer Processes for MIME han
Rule ID: SV-16413r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI594
Rule Title: Internet Explorer Processes for MIME handling is not enabled. IExplore

Vulnerability Discussion: Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. The Consistent MIME Handling\Internet Explorer Processes policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data provided by the file. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistent and properly labeled helps prevent malicious file downloads from infecting your network. Therefore, this appendix recommends you configure this policy as Enabled for all environments specified in this guide.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Consistent Mime Handling -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_HANDLING

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15568
Group Title: DTBI599 - Internet Explorer Processes for MK proto
Rule ID: SV-16415r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI599
Rule Title: Internet Explorer Processes for MK protocol is not enabled. (Reserved)

Vulnerability Discussion: The MK Protocol Security Restriction policy setting reduces attack surface area by blocking the seldom used MK protocol. Some older Web applications use the MK protocol to retrieve information from compressed files. Setting this policy to Enabled blocks the MK protocol for Windows Explorer and Internet Explorer, which causes resources that use the MK protocol to fail. Disabling this setting allows applications to use the MK protocol API. Because the MK protocol is not widely used, it should be blocked wherever it is not needed. This appendix recommends you configure this setting to Enabled to block the MK protocol unless you specifically need it in your environment. Note: Because resources that use the MK protocol will fail when you deploy this setting, you should ensure that none of your applications use the MK protocol.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL

Criteria: If the value (reserved) is REG_SZ = 1, this is not a finding

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> MK Protocol Security Restriction -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_DISABLE_MK_PROTOCOL

Criteria: Set the value (reserved) to REG_SZ = 1.

Group ID (Vulid): V-15569
Group Title: DTBI612 - Internet Explorer Processes for Zone Ele
Rule ID: SV-16416r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI612

Rule Title: Internet Explorer Processes for Zone Elevation is not enabled. Explorer

Vulnerability Discussion: Internet Explorer places restrictions on each Web page it opens that are dependent upon the location of the Web page (such as Internet zone, Intranet zone, or Local Machine zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine zone, which makes the Local Machine security zone a prime target for malicious attackers. If you enable this policy setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach stops content running in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes. Because of the severity and relative frequency of zone elevation attacks, this appendix recommends that you configure this setting as Enabled in all environments.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15570
Group Title: DTBI614 - Internet Explorer Processes for Zone Ele
Rule ID: SV-16417r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI614
Rule Title: Internet Explorer Processes for Zone Elevation is not enabled. IExplore

Vulnerability Discussion: Internet Explorer places restrictions on each Web page it opens that are dependent upon the location of the Web page (such as Internet zone, Intranet zone, or Local Machine zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine zone, which makes the Local Machine security zone a prime target for malicious attackers. If you enable this policy setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach stops content running in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes. Because of the severity and relative frequency of zone elevation attacks, this appendix recommends that you configure this setting as Enabled in all environments.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Protection From Zone Elevation -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ZONE_ELEVATION

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15571
Group Title: DTBI647 - Internet Explorer Processes for restrict
Rule ID: SV-16418r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI647
Rule Title: Internet Explorer Processes for restricting pop-up windows is not enabled. Explorer

Vulnerability Discussion: Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. Often, disreputable Web sites will resize windows to either hide other windows or force you to interact with a window that contains malicious code. The Scripted Window Security Restrictions security feature restricts pop-up windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or hide other windows’ title and status bars. If you enable the Scripted Window Security Restrictions\Internet Explorer Processes policy setting, pop-up windows and other restrictions apply for Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts can continue to create pop-up windows and windows that hide other windows. This appendix recommends you configure this setting to Enabled to help prevent malicious Web sites from controlling your Internet Explorer windows or fooling users into clicking on the wrong window.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components ->

Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

Criteria: Set the value explorer.exe to REG_SZ = 1.

Group ID (Vulid): V-15572
Group Title: DTBI649 - Internet Explorer Processes for restrict
Rule ID: SV-16419r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI649
Rule Title: Internet Explorer Processes for restricting pop-up windows is not enabled. IExplorer

Vulnerability Discussion: Internet Explorer allows scripts to programmatically open, resize, and reposition various types of windows. Often, disreputable Web sites will resize windows to either hide other windows or force you to interact with a window that contains malicious code. The Scripted Window Security Restrictions security feature restricts pop-up windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or hide other windows’ title and status bars. If you enable the Scripted Window Security Restrictions\Internet Explorer Processes policy setting, pop-up windows and other restrictions apply for Windows Explorer and Internet Explorer processes. If you disable or do not configure this policy setting, scripts can continue to create pop-up windows and windows that hide other windows. This appendix recommends you configure this setting to Enabled to help prevent malicious Web sites from controlling your Internet Explorer windows or fooling users into clicking on the wrong window.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Scripted Window Security Restrictions -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WINDOW_RESTRICTIONS

Criteria: Set the value iexplore.exe to REG_SZ = 1.

Group ID (Vulid): V-15573
Group Title: DTBI685 - Configure Outlook Express is not disable
Rule ID: SV-16420r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI685
Rule Title: Configure Outlook Express is not disabled.

Vulnerability Discussion: The Configure Outlook Express setting allows administrators to enable and disable the ability for Microsoft Outlook® Express users to save or open attachments that can potentially contain a virus. Selecting the block attachments option of this setting prevents users opening or saving attachments to e – mail that could potentially contain a virus.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Configure Outlook Express" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Microsoft\Outlook Express

Criteria: If the value BlockExeAttachments is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Configure Outlook Express" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Microsoft\Outlook Express

Criteria:Set the value BlockExeAttachments to REG_DWORD = 0.

Group ID (Vulid): V-15574
Group Title: DTBI690 - Disable AutoComplete for forms is not en
Rule ID: SV-16421r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI690
Rule Title: Disable AutoComplete for forms is not enabled.

Vulnerability Discussion: This AutoComplete feature suggests possible matches when users are filling up forms. If you enable this setting, the user is not suggested matches when filling forms. The user cannot change it. If you disable this setting, the user is suggested possible matches when filling forms. The user cannot change it.
If you do not configure this setting, the user has the freedom to turn on the auto-complete feature for forms. To display this option, the users open the Internet Options dialog box, click the Contents Tab and click the Settings button.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable AutoComplete for forms" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: If the value Use FormSuggest is REG_SZ = no, this is not a finding.

HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: If the value FormSuggest is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable AutoComplete for forms" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Set the value Use FormSuggest to REG_SZ = no.

HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: Set the value FormSuggest to REG_DWORD = 1.

Group ID (Vulid): V-15575
Group Title: DTBI695 - Disable external branding of Internet Ex
Rule ID: SV-16422r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI695
Rule Title: Disable external branding of Internet Explorer is not enabled.

Vulnerability Discussion: Prevents branding of Internet programs, such as customization of Internet Explorer and Outlook Express logos and title bars, by another party. If you enable this policy, it prevents customization of the browser by another party, such as an Internet service provider or Internet content provider. If you disable this policy or do not configure it, users could install customizations from another party-for example, when signing up for Internet services. This policy is intended for administrators who want to maintain a consistent browser across an organization.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable external branding of Internet Explorer" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions

Criteria: If the value NoExternalBranding is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable external branding of Internet Explorer" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions

Criteria: Set the value NoExternalBranding to REG_DWORD = 1.

Group ID (Vulid): V-15577
Group Title: DTBI705 - Disable the Reset Web Settings feature i
Rule ID: SV-16424r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI705
Rule Title: Disable the Reset Web Settings feature is not enabled.

Vulnerability Discussion: Prevents users from restoring default settings for home and search pages.
If you enable this policy, the Reset Web Settings button on the Programs tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can restore the default settings for home and search pages. The "Disable the Programs page" policy (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the Programs tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable the Reset Web Settings feature" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: If the value ResetWebSettings is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable the Reset Web Settings feature" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: Set the value ResetWebSettings to REG_DWORD = 1.

Group ID (Vulid): V-15579
Group Title: DTBI715 - Turn off Crash Detection is not enabled.
Rule ID: SV-16426r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI715

Rule Title: Turn off Crash Detection is not enabled.

Vulnerability Discussion: The Turn off Crash Detection policy setting allows you to manage the crash detection feature of add-on management in Internet Explorer. If you enable this policy setting, a crash in Internet Explorer will be similar to one on a computer running Windows XP Professional Service Pack 1 and earlier: Windows Error Reporting will be invoked. If you disable this policy setting, the crash detection feature in add-on management will be functional. Because Internet Explorer crash report information could contain sensitive information from the computer's memory, this appendix recommends you configure this option to Enabled unless you are experiencing frequent repeated crashes and need to report them for follow-up troubleshooting. In those cases you could temporarily configure the setting to Disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Crash Detection" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions

Criteria: If the value NoCrashDetection is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn off Crash Detection" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions

Criteria:Set the value NoCrashDetection to REG_DWORD = 1.

Group ID (Vulid): V-15580
Group Title: DTBI720 - Turn off page transitions is not enabled
Rule ID: SV-16427r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI720
Rule Title: Turn off page transitions is not enabled.

Vulnerability Discussion: This policy setting specifies if, as you move from one Web page to another, Internet Explorer fades out of the page you are leaving and fades into the page to which you are going. If you enable this policy setting, page transitions will be turned off. The user cannot change this behavior. If you disable this policy setting, page transitions will be turned on. The user cannot change this behavior. If you do not configure this policy setting, the user can turn on or off page transitions.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Browsing -> "Turn off page transitions" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: If the value Page_Transitions is REG_DWORD = 0, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Browsing -> "Turn off page transitions" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Set the value Page_Transitions to REG_DWORD = 0.

Group ID (Vulid): V-15581
Group Title: DTBI725 - Turn on the auto-complete feature for us
Rule ID: SV-16428r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI725
Rule Title: Turn on the auto-complete feature for user names and passwords on forms are not disabled.

Vulnerability Discussion: This AutoComplete feature can remember and suggest User names and passwords on Forms. If you enable this setting, the user cannot change "User name and passwords on forms" or "prompt me to save passwords". The Auto Complete feature for User names and passwords on Forms will be turned on. You have to decide whether to select "prompt me to save passwords". If you disable this setting the user cannot change "User name and passwords on forms" or "prompt me to save passwords". The Auto Complete feature for User names and passwords on Forms is turned off. The user also cannot opt to be prompted to save passwords. If you do not configure this setting, the user has the freedom of turning on Auto complete for User name and passwords on forms and the option of prompting to save passwords. To display this option, the users open the Internet Options dialog box, click the Contents Tab and click the Settings button.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn on the auto-complete feature for user names and passwords on forms" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: If the value FormSuggest Passwords is REG_SZ = no, this is not a finding.

HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: If the value FormSuggest Passwords is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Turn on the auto-complete feature for user names and passwords on forms" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Set the value FormSuggest Passwords to REG_SZ = no.

HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: Set the value FormSuggest Passwords to REG_DWORD = 1.

Group ID (Vulid): V-15582
Group Title: DTBI730 - Turn on the Internet Connection Wizard A
Rule ID: SV-16429r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI730
Rule Title: Turn on the Internet Connection Wizard Auto Detect is not disabled.

Vulnerability Discussion: This policy setting determines if the Internet Connection Wizard was completed. If it was not completed, it launches the Internet Connection Wizard. If you enable this policy setting, the Internet Connection Wizard is launched automatically if it was not completed before. The user cannot prevent the wizard from launching. If you disable this policy setting, the Internet Connection Wizard is not launched automatically. The user can launch the wizard manually. If you do not configure this policy setting, the user will have the freedom to decide whether the Internet Connection Wizard should be launched automatically.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Internet Connection Wizard Settings -> "Turn on the Internet Connection Wizard Auto Detect" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Connection Wizard

Criteria: If the value DisableICW is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for User Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Settings -> Advanced Settings -> Internet Connection Wizard Settings -> "Turn on the Internet Connection Wizard Auto Detect" will be set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Internet Connection Wizard

Criteria: Set the value DisableICW to REG_DWORD = 1.

Group ID (Vulid): V-15603
Group Title: DTBI596 - IE Processes for MIME sniffing is n
Rule ID: SV-16492r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI596

Rule Title: Internet Explorer Processes for MIME sniffing is not enabled. Explorer

Vulnerability Discussion: MIME sniffing is the process of examining the content of a MIME file to determine its context — whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When set to Enabled, MIME sniffing will never promote a file of one type to a more dangerous file type. Disabling MIME sniffing configures Internet Explorer processes to allow a MIME sniff that promotes a file of one type to a more dangerous file type. For example, promoting a text file to an executable file is a dangerous promotion because any code in the supposed text file would be executed. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistently handled helps prevent malicious file downloads from infecting your network. Therefore, this appendix recommends you configure this policy as Enabled for all environments specified in this guide. Note: This setting works in conjunction with, but does not replace, the Consistent MIME handling settings.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value explorer.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value explorer.exe is REG_SZ = 1.

Group ID (Vulid): V-15604
Group Title: DTBI597 - Internet Explorer Processes for MIME sni
Rule ID: SV-16493r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI597
Rule Title: Internet Explorer Processes for MIME sniffing is not enabled. IExplore

Vulnerability Discussion: MIME sniffing is the process of examining the content of a MIME file to determine its context — whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. When set to Enabled, MIME sniffing will never promote a file of one type to a more dangerous file type. Disabling MIME sniffing configures Internet Explorer processes to allow a MIME sniff that promotes a file of one type to a more dangerous file type. For example, promoting a text file to an executable file is a dangerous promotion because any code in the supposed text file would be executed. MIME file-type spoofing is a potential threat to your organization. Ensuring that these files are consistently handled helps prevent malicious file downloads from infecting your network. Therefore, this appendix recommends you configure this policy as Enabled for all environments specified in this guide. Note: This setting works in conjunction with, but does not replace, the Consistent MIME handling settings.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value iexplore.exe is REG_SZ = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Security Features -> Mime Sniffing Safety Feature -> "Internet Explorer Processes" will be set to “Enabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_SNIFFING

Criteria: If the value iexplore.exe is REG_SZ = 1.

Group ID (Vulid): V-16879
Group Title: DTBI025 - The Download signed ActiveX controls pro
Rule ID: SV-17879r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI025
Rule Title: The Download signed ActiveX controls property is not set properly for the Lockdown Zone.

Vulnerability Discussion: This policy setting allows you to manage whether users may download signed ActiveX controls from a page in the zone. If you enable this policy, users can download signed controls without user intervention. If you select Prompt in the drop-down box, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded. If you disable the policy setting, signed controls cannot be downloaded. If you do not configure this policy setting, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3

Criteria: If the value 1001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3

Criteria: Set the value 1001 to REG_DWORD = 3.

Group ID (Vulid): V-17296
Group Title: DTBI010 - Prevent performance of First Run Customi
Rule ID: SV-18332r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI010
Rule Title: Prevent performance of First Run Customize settings is not enabled.

Vulnerability Discussion: This policy setting prevents performance of the First Run Customize settings ability and controls what the user will see when they launch Internet Explorer for the first time after installation of Internet Explorer.
If you enable this policy setting, users must make one of two choices:
1: Skip Customize Settings, and go directly to the user’s home page.
2: Skip Customize Settings, and go directly to the "Welcome to Internet Explorer" Web page.
If you disable or do not configure this policy setting, users go through the regular first run process.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent performance of First Run Customize settings" will be set to “Enabled” and "Go directly to home page" selected.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: If the value DisableFirstRunCustomize is REG_DWORD = 1, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Prevent performance of First Run Customize settings" will be set to “Enabled” and "Go directly to home page" selected.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Main

Criteria: Set the value DisableFirstRunCustomize is REG_DWORD = 1.

Group ID (Vulid): V-21887
Group Title: History setting is not enabled or set to 40 days.
Rule ID: SV-24724r1_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI300
Rule Title: Disable Configuring History - Histroy setting is not set to 40 days.

Vulnerability Discussion: This setting specifies the number of days that Internet Explorer keeps track of the pages viewed in the History List. The delete Browsing History option can be accessed using Tools, Internet Options and General tab. It is also available as Delete History directly under tools, Internet options, Delete Browsing History in Internet Explorer 7. If you enable this policy setting, a user cannot set the number of days that Internet Explorer keeps track of the pages viewed in the History List. You must specify the number of days that Internet Explorer keeps track of the pages viewed in the History List. Users will not be able to delete browsing history. If you disable or do not configure this policy setting, a user can set the number of days that Internet Explorer keeps track of the pages viewed in the History List and has the freedom to Delete Browsing History.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable "Configuring History" " will be set to “Enabled” and "40" entered in 'Days to keep pages in History'.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: If the value History is REG_DWORD = 1, this is not a finding.

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Url History

Criteria: If the value DaysToKeep is REG_DWORD = 40 (decimal), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> "Disable "Configuring History" " will be set to “Enabled” and "40" entered in 'Days to keep pages in History'.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: Set the value History to REG_DWORD = 1.

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Url History

Criteria: Set the value DaysToKeep to REG_DWORD = 40 (decimal).